Notice of Allowability	Application No.	Applicant(s)	
	09/725,272	IMAI ET AL.	
	Examiner	Art Unit	
	Minh Dieu Nguyen	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *September 20, 2004*.

2. ☒ The allowed claim(s) is/are *14-17,20-23,25-30,32-35 and 38-40*.

3. ☒ The drawings filed on *29 November 2000* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *Attached* .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Phil Miller on 2/14/05.

2. The application has been amended as follows:

Please amend the claims as specified on page 3.

AMENDMENTS TO THE CLAIMS:

1.-13. (Canceled)

14. (Previously presented) A center computer in a digital signature system, comprising:

first generating means for generating a signing-key for a signer;

second generating means for generating a verification-key for a verifier;

a first output device outputting the signing-key generated by the first generating means; and

a second output device outputting the verification-key generated by the second generating means, wherein:

the first generating means comprises means for generating a first multivariate function, and means for generating a second multivariate function obtained by substituting the signer's identification code into a first variable of the first multivariate function;

the first output device outputs the second multivariate function as the signing-key for the signer;

the second generating means comprises means for generating a random number, a third multivariate function obtained by substituting the random number to a second variable of the first multivariate function; and

the second output device outputs the random number and the third multivariate function as the verification-key for the verifier.

15. (Original) The center computer according to claim 14, wherein:

the second multivariate function is generated by substituting the signer's identification code into a first group of variables of the first multivariate function.

16. (Original) The center computer according to claim 14, wherein:

a group of random numbers is generated and the third multivariate function is generated by substituting the group of random numbers into a second group of variables of the first multivariate function; and

the group of random numbers and the third multivariate function are outputted as the verification-key for the verifier.

17. (Currently amended) A method of establishing a signing-key for a signer and a verification-key for a verifier, said method comprising:

in a computer of a digital signature system,

generating a first multivariate function;

generating a second multivariate function obtained by substituting a signer's identification code into a first variable of the first multivariate function;

outputting the second multivariate function as a signing-key for the signer;

generating a random number, a third multivariate function obtained by substituting the random number into a second variable of the first multivariate function; and

outputting the random number and the third multivariate function as a verification-key for the verifier.

18.-19. (Canceled)

20. (Previously presented) A computer readable recording medium having a program recorded thereon, the program controlling the computer so as to:

generate a first multivariate function;

generate a second multivariate function obtained by substituting a signer's identification code into a first variable of the first multivariate function;

output the second multivariate function as a signing-key for the signer;

generate a random number, a third multivariate function obtained by substituting the random number to a second variable of the first multivariate function; and

output the random number and the third multivariate function as a verification-key for a verifier.

21. (Original) The computer readable recording medium according to claim 20, wherein the program controls the computer so as to:

generate the second multivariate function by substituting the signer's identification code into a first group of variables of the first multivariate function; and

output the second multivariate function as a signing-key for the signer.

22. (Original) The computer readable recording medium according to claim 20, wherein the program controls the computer so as to:

generate a group of random numbers and generate a third multivariate function by substituting the group of random numbers into a second group of variables of the first multivariate function; and

output the group of random numbers and the third multivariate function as a

verification-key for the verifier.

23. (Previously presented) A method of establishing a digital signature in a digital signature system comprising a center computer and a first and second terminal devices which can communicate with each other, comprising:

in the center computer,

generating a first multivariate function,

generating a second multivariate function obtained by substituting a signer's identification code into a first variable of the first multivariate function,

outputting the second multivariate function as a signing-key for the signer,

generating a random number, a third multivariate function obtained by substituting the random number into a second variable of the first multivariate ~~function,~~ function; and

outputting the random number and the third multivariate function as a verification-key for a verifier;

in the first terminal device,

accepting the signer's signing-key;

inputting the accepted signer's signing-key;

inputting an identification code of a digital data;

generating a fourth multivariate function obtained by substituting the identification code of the digital data into the third variable of the second multivariate function; and

outputting the fourth multivariate function as a digital signature;

in the second terminal device,

accepting the verification-key,

inputting the accepted verifier's verification-key,

accepting an identity of the signer,

inputting the signer's identification code,

accepting the identification code of the digital data,

inputting the accepted identification code of the digital data,

accepting the digital signature,

inputting the accepted digital signature,

generating a first evaluation value by substituting the random number into the second variable of the fourth multivariate function,

generating a second evaluation value by substituting the signer's identification code and the identification code of the digital data into the first and third variables of the third multivariate function, respectively, and

accepting the digital signature as valid if both of the first and second evaluation values equal, and otherwise rejecting the digital signature as invalid.

24. (Canceled)

25. (Previously presented) A first terminal device in a digital signature system, comprising:

accepting means for accepting a signer's signing-key;

a first input device inputting the signer's signing-key;

a second input device inputting an identification code of a digital data;

generating means for generating a digital signature; and

an output device outputting the digital signature generated by the generating means, wherein:

the digital signature generating means generates a fourth multivariate function obtained by substituting an identification code of a digital data into a third variable of a second multivariate function; and

the output device outputs the fourth multivariate function as the digital signature.

26. (Original) The first terminal device according to claim 25, wherein:

the digital signature generating means generates a fourth multivariate function by substituting an identification code of a digital data into a third group of variables of a second multivariate function; and

the output device outputs the fourth multivariate function as the digital signature.

27. (Currently amended) A method of establishing a digital signature comprising:

in a terminal device of a digital signature system,

accepting a signer's signing-key;

inputting the accepted signer's signing-key;

inputting an identification code of a digital data;

generating a fourth multivariate function of a plurality of multivariate functions obtained by substituting the identification code of the digital data into a third variable of a second multivariate function; and

outputting the fourth multivariate function as a digital signature.

28. (Previously presented) The method of establishing a digital signature according to claim 27, wherein:

a fourth multivariate function is generated by substituting an identification code of a digital data into a third group of variables of a second multivariate function; and

the fourth multivariate function is outputted as a digital signature.

29. (Previously presented) A computer readable recording medium having a program recorded thereon, the program controlling a computer so as to:

accept an inputted signer's signing-key;

accept an inputted identification code of a digital data;

generate a fourth multivariate function of a plurality of multivariate functions obtained by substituting the identification code of the digital data into a third variable of a second multivariate function; and

output the fourth multivariate function as a digital signature.

30. (Previously presented) The computer readable recording medium according to claim 29, wherein the program controls the computer so as to:

generate the fourth multivariate function by substituting the identification code of the digital data into a third group of variables of the second multivariate function; and

output the fourth multivariate function as a digital signature.

31. (Canceled)

32. (Previously presented) A second terminal device in a digital signature system

comprising:

first accepting means for accepting a verification-key;

a first input device inputting a verifier's verification-key;

second accepting means for accepting a signer's identity;

a second input device inputting the signer's identification code;

third accepting means for an identification code of a digital data;

a third input device inputting the identification code of the digital data;

fourth accepting means for accepting a digital signature;

a fourth input device inputting the digital signature;

verifying means for verifying a validity of the digital signature using the verification-key, the signer's identification code and the identification code of the digital data;

an output device outputting the result of verifying the validity of the digital signature, namely, acceptable as valid or not, wherein the verifying means for verifying the validity of the digital signature:

generates a first evaluation value by substituting a random number into a second variable of a fourth multivariate function of a plurality of multivariate functions;

generates a second evaluation value by substituting the signer's identification code and the identification code of the digital data into a first variable and a third variable of a third multivariate function, respectively; and

accepts the digital signature as valid if both of the first and second evaluation values equal, and otherwise rejects the digital signature as invalid.

33. (Original) The second terminal device according to claim 32, wherein a first evaluation value is generated by substituting a group of random numbers into a second group

of variables of the fourth multivariate function.

34. (Original) The second terminal device according to claim 32, wherein the signer's identification code is substituted into a first group of variables of the third multivariate function, or the identification code of the digital data is substituted into a third group of variables of the third multivariate function.

35. (Currently amended) A method of verifying the validity of a digital signature comprising:

in a terminal device of a digital signature system,

accepting a verifier's verification-key;

inputting the accepted verification-key;

accepting a signer's identity;

inputting the signer's identification code;

accepting an identification code of a digital data;

inputting the identification code of the digital data;

accepting a digital signature;

inputting the digital signature;

generating a first evaluation value by substituting a random number into a second variable of a fourth multivariate function of a plurality of multivariate functions;

generating a second evaluation value by substituting the signer's identification code and the identification code of the digital data into a first variable and a third variable of a third multivariate function, respectively; and

accepting the digital signature as valid if both of the first and second evaluation values

equal, and otherwise rejecting the digital signature as invalid.

36.-37. (Canceled)

38. (Previously presented) A computer readable recording medium having a program recorded thereon, the program controlling the computer so as to:

accept an inputted verifier's verification-key;

accept an inputted signer's identification code;

accept an inputted identification code of a digital data;

accept an inputted digital signature;

generate a first evaluation value by substituting a random number into a second variable of a fourth multivariate function of a plurality of multivariate functions;;

generate a second evaluation value by substituting the signer's identification code and the identification code of the digital data into a first variable and a third variable of a third multivariate function, respectively; and

accept the digital signature as valid if both of the first and second evaluation values equal, and otherwise reject the digital signature as invalid.

39. (Original) The computer readable recording medium according to claim 38, wherein the program controls the computer so as to generate a first evaluation value by substituting a group of random numbers into a second group of variables of the fourth multivariate function.

40. (Original) The computer readable recording medium according to claim 38,

wherein the program controls the computer so as to substitute the signer's identification code into a first group of variables of the third multivariate function, or substitute the identification code of the digital data into a third group of variables of the third multivariate function.

41.-82. (Canceled)

Allowable Subject Matter

3. The communication dated September 20, 2004 with the cancellation of claims 1-13, 18-19, 24, 31, 36-37 and 41-82, and the amendment of claims 14, 17-18, 20-23, 28-30, 35 and 38-40 has been fully considered.

4. Claims 14-17, 20-23, 25-30, 32-35, 38-40 are allowed.

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on 571-272-3868. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Minh Dieu Nguyen
Examiner
Art Unit 2137

mdn
2/22/05

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER